

CHAPTER 2

SECURITY

SECURITY DEFINED

In this chapter, we will discuss the physical security provided to all mail and the Navy Information and Personnel Security Program as it applies to classified material sent in the mail. We will also discuss the requirements for maintaining the security of mail and equipment, random inspections, probable cause searches, and instructions on what to do if a suspected letter or parcel bomb is found.

The word security has two meanings. The first meaning applies to the internal and external security provided to all mail. This means that when you or anyone else entrusts an article to the postal system, you can depend on it arriving at its destination safely and securely.

The Military Postal Service (MPS) and the U.S. Postal Service (USPS) rank second to none in the security given to mail articles that are accepted for delivery. The privacy to which every letter and parcel is entitled is established by law, and certain articles—specifically, registered and insured mail—are given special protection against loss or damage.

The second meaning of the word security applies to transmitting classified material through the postal system. The relative safety from compromise is amply illustrated by the fact that certain classified matter is transmitted regularly through registered mail channels.

Q1. Which agencies are rated as second to none in providing security for military mail?

GENERAL SECURITY PROCEDURES

Security of the mail is a command responsibility. Mail consigned for transmission is always delivered into the hands of a responsible postal agency, military or commercial carrier, or the authorized agents of these carriers who can make a reasonable guarantee of onward transmission to achieve ultimate delivery as intended. You should never turn mail over to a haphazard or makeshift means of transmission.

In general, registered military mail may be transported outside the Continental United States (CONUS) and Canada, only in U.S. flag certified cargo air carriers, and while in U.S. custody or control. Military mail dispatching agents are responsible for the security regulations covering the mail route for which they are responsible as well as the next onward transfer point. Where it appears that security regulations will not be met, the dispatching agent will withdraw the registered mail from transmission and request instructions from the consigning agency.

Official mail containing classified material transmitted outside CONUS should arrive safely at its destination if the following conditions are met:

- Prepared properly
- Addressed properly with complete and correct mailing address as contained in the *Standard Navy Distribution List* (SNDL), OPNAV N09B22
- Acceptance as registered mail into the U.S. domestic postal system in CONUS
- Acceptance as registered mail into the military postal system overseas
- Observed for prescribed controls and safeguards

The *Department of the Navy Information and Personnel Security Program Regulation*, OPNAVINST 5510.1, provides all Navy activities and personnel with detailed regulations and guidance for classifying, marking, handling, and methods of transmission of classified material.

Q2. What type of air carrier is used to transport registered mail outside CONUS and Canada?

MAIL CENTER KEYS

The number of keys to the mail center should be kept to a minimum. The OMM will maintain accountability of all keys held by others.

As the Official Mail Manager (OMM), you are responsible for your key and for informing your assistants of their responsibilities for the keys assigned to them.

In larger offices there may be an extra key used by duty personnel. This key is controlled at all times by a daily log fixing the responsibility and accountability of the person holding the duty key. Each duplicates key and copies of combinations are placed in a Duplicate Key Envelope, PS Form 3977 (fig. 2-1), SF 700 (fig. 2-2), or a similar type of envelope, sealed and endorsed by the custodian of the key, and placed in the CO's or an appointed official's safe.

Q3. Before placing keys in a security container, the extra keys are placed in what types of envelopes?


COMBINATIONS

You should change safe combinations when the following conditions are present:

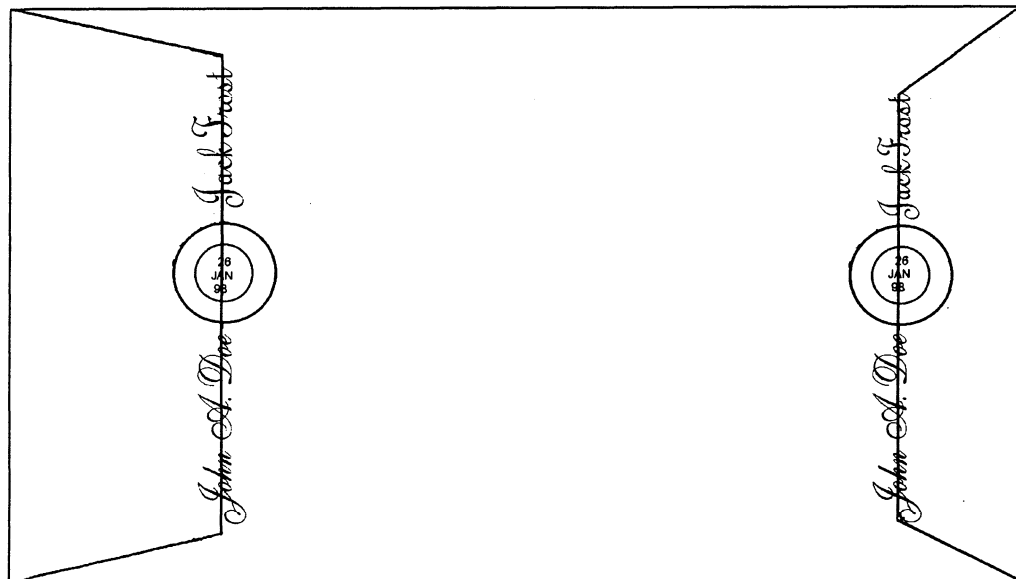
- When the safe is received initially
- Whenever a possible compromise of the combination has occurred
- When personnel having knowledge of combinations are transferred out of the activity or relieved of their duties
- At least annually

When combination numbers are selected, multiples of five or simple ascending or descending arithmetical series should be avoided.

Q4. At least how often should safe combinations be changed?

 Duplicate Key Inventory				Instructions See Section 362, Handbook F-1, Post Office Accounting Procedures <small>After the duplicate keys are enclosed and the flap is sealed, both you (the employee to whom the keys are assigned) and the witness to the sealing of this envelope must sign across both flaps on the reverse of this envelope. Affix a distinct and legible postmark across both envelope flaps. Give this signed and postmarked envelope to the appropriate supervisor who will be personally responsible for its protection.</small> <small>If it is necessary for you to withdraw keys temporarily, open this envelope in the presence of a witness. Cut along one end, leaving the signatures and postmarks intact. Both you and the witness must endorse and date the envelope. When the keys are returned, discard the opened envelope and prepare a new envelope.</small> <small>If access to one of your locked receptacles is necessary while you are absent from duty, the appropriate supervisor will remove the key from this envelope in the presence of a designated witness and both will endorse and date this envelope and show reason for withdrawing the key. The supervisor (or designee) and the witness must inventory the contents of the receptacle and certify the inventory. The supervisor must maintain the inventory with the opened envelope.</small>
Employee Name (Print Last, First, & MI) FROST, JACK R.				
Operating Unit USS CARNEY (DDG-64)				
Receptacle	No.	No. Keys	Serial No.	
Cash Drawer	3	1	0031	
Stamp Cabinet				
Safe Compartment				
Envelope Drawer				
Designated Witness Name (Print) JOHN A. DOE				
Designated Witness Name (Print) JOHN A. DOE				

PS Form 3977, April 1988



OMMPC004

Figure 2-1.—Duplicate Key Envelope, PS Form 3977, showing completed front and back.

SECURITY CONTAINER INFORMATION INSTRUCTIONS 1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP). 2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER. 3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER. 4. DETACH PART 2A AND INSERT IN ENVELOPE. 5. SEE PRIVACY ACT STATEMENT ON REVERSE.			1. AREA OR POST (if required)	2. BUILDING (if required)	3. ROOM NO.
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)			5. CONTAINER NO.		
6. MFG & TYPE CONTAINER		7. MFG & TYPE LOCK		8. DATE COMBINATION CHANGED	
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE					
10. Immediately notify one of the following persons, if this container is found open and unattached.					
EMPLOYEE NAME	HOME ADDRESS		HOME PHONE		

1. ATTACH TO INSIDE OF CONTAINER

700-101
NSN 7540-01-214-5372

STANDARD FORM 700 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

WARNING
 WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CONTAINER NUMBER _____

COMBINATION

_____ turns to the (right) (left) stop at _____

_____ turns to the (right) (left) stop at _____

_____ turns to the (right) (left) stop at _____

_____ turns to the (right) (left) stop at _____

WARNING
THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED

UNCLASSIFIED UPON CHANGE OF COMBINATION

2A INSERT IN ENVELOPE

SF 700 (8-85)
Prescribed by
GSA/ISOO
32 CFR 2003

OMMPC005

Figure 2-2. — Security Container Envelope, SF 700

INTERIOR SECURITY

All personnel who are not directly involved with the handling of official mail must be prohibited entry to the office working space. The only exceptions to this rule are the commanding officer (CO), executive officer (XO), and those personnel who are members of an official inspecting party while carrying out assigned duties. If the office operates on a 24-hour basis, off-duty personnel should be excluded. When a working party is required to handle mail, the members of the working party may be authorized entry to the working space while closed mailbags are being handled. Supervision will always be provided while the working party is handling the mail.

MAIL BOMBS

Because of an increase in worldwide terrorist activities, we must not laugh at the myth of letter bombs. You, as the OMM, could very well be in the position to determine what to do in a crisis situation to increase present awareness and also to provide guidance in identifying suspected mail bombs. The information listed below should be disseminated among your personnel. Figure 2-3 shows an example of a letter bomb.

Keep in mind that a bomb can be enclosed in either a parcel or an envelope. There is no set pattern of the outward appearance of the parcel or envelope. The form of a letter bomb is limited only by the imagination of the sender. Mail bombs will usually have unique characteristics. Some of these characteristics are listed as follows:

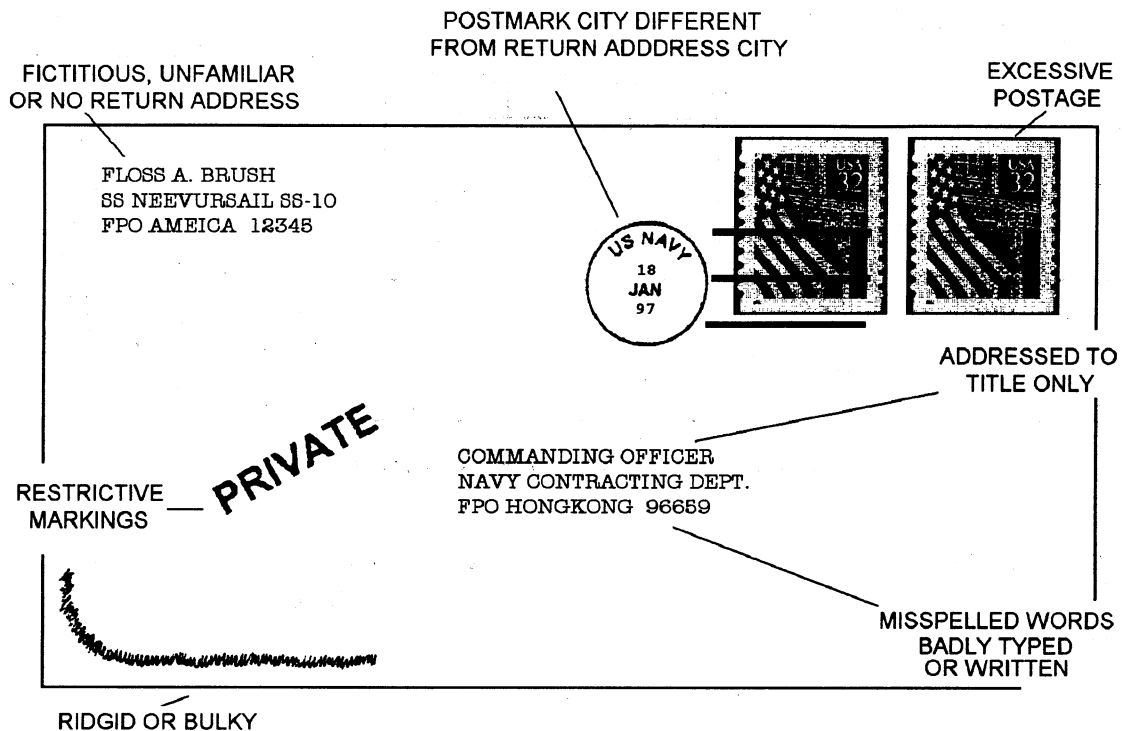
Mail bombs may bear restricted endorsements such as Personal or Private.

- The addressee's name and/or title may be inaccurate.
- Mail bombs may reflect distorted handwriting or the name and address may be prepared with homemade labels or cut-and-paste lettering.
- Mail bombs may have protruding wires, aluminum foil, or oil stains visible and may emit a peculiar odor.
- Mail bombs may have an excessive amount of postage stamps affixed.
- Letter-type bombs may feel rigid or appear uneven or lopsided.
- Parcel bombs may be unprofessionally wrapped with several combinations of tape used to secure the package and may be endorsed **Fragile—Handle with Care or Rush—Do Not Delay**.
- Parcel bombs may make a buzzing or ticking noise, or a sloshing sound.

Pressure or resistance may be noted when removing contents from an envelope or parcel (fig. 2-4).

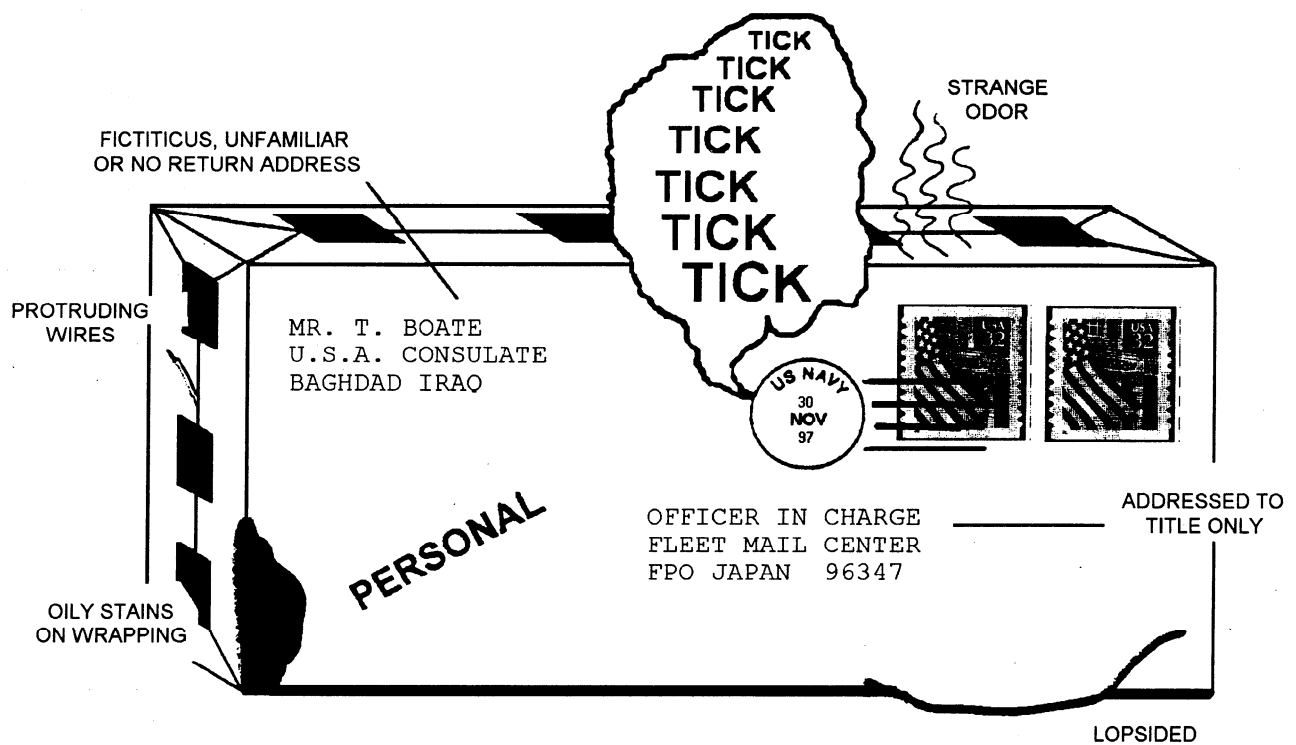
If you discover or are suspicious of a piece of mail and are unable to reasonably verify the contents, you should take the following actions:

- **DO NOT OPEN.**
- Isolate the article and evacuate the area immediately.



OMMPC006

Figure 2-3.—Example of a letter bomb.



OMMPC007

Figure 2-4.—Example of a parcel bomb.

- Do not put the article in a bucket of water or a confined space such as a desk drawer or file cabinet.

If time allows, open windows in the immediate area. This will help to clear the air of potentially explosive gases.

It is your job to explain to your personnel that if they have any reason to be suspicious of a letter or parcel, they must react immediately.

Make sure your personnel take NO chances or worry about possible embarrassment if the article turns out to be harmless.

You should immediately contact the appropriate officials for assistance.

For handling and reporting articles reasonably suspected of being dangerous to persons or suspected as letter bombs, refer to the *Department of Defense Postal Manual*, DOD 4525.6-M, Volume 2, chapter 3.

Q5. A bomb could be enclosed in what two basic types of packaging?

Q6. For the handling and reporting of articles suspected of containing bombs, you should refer to what publication?

REGISTERED MAIL

As the official mail manager, you are responsible for the security and accountability of handling registered mail. When registered mail transits through your facility for further transfer (FFT) to the post office, complete accountability, proper documentation, and the utmost security are mandatory.

Official registered mail transmitted within U.S. military postal channels outside CONUS is treated as if it contained classified material.

You should ensure that the people who handle registered mail keep the mail under constant surveillance or lock it in a safe or vault until a receipt has been obtained. Registered mail must be kept separate from ordinary mail and given special protection from accident or theft.

Mail center personnel handling registered mail must account for each piece by preparing a Registered Mail Balance and Inventory Sheet (DD Form 2261) at the end of a shift or work day.

SECURITY OF CLASSIFIED MATERIAL

You may come in contact with classified material in the performance of your duties. Normally, you will not actually handle classified material except as registered mail, but you will be expected to have some knowledge of the categories of classified material and the rules of security to perform your job properly. You should be able to recognize classified material and know what to do—or not to do—with it.

NAVY INFORMATION AND PERSONNEL SECURITY PROGRAM

The chain of responsibility for the Navy Information and Personnel Security Program within the Navy begins with the Secretary of the Navy (SECNAV), who is responsible to the Secretary of Defense (SECDEF) for establishing and maintaining the program and complying with all the directives regarding protection of classified information. The basic directive is the *Department of the Navy Information and Personnel Security Program Regulation*, OPNAVINST 5510.1, which incorporates requirements levied by executive orders, National Security Council directives, and public laws. Other directives, including *United States Navy Regulations, 1990*, and general orders, shape the security program in the Navy.

SECNAV has made the Chief of Naval Operations (CNO) responsible for policies regarding the security of classified information. The CNO has designated the Director of Naval Intelligence (OP-09N) as the official primarily responsible for seeing that an effective program exists that follows all the directives issued by higher authority. COs are responsible to the Director of Naval Intelligence for carrying out the Navy Information and Personnel Security Program in their commands. The security manager is designated by the CO as the direct representative in all matters affecting the security of classified information, and is charged with the responsibility for the administration of the program. Finally, every individual who has access to classified information is responsible for protecting that information according to the OPNAVINST 5510.1.

Q7. Policies relating to the security of Department of the Navy classified information is the responsibility of what official?

PURPOSE OF SECURITY PROGRAM

The purpose of the Navy's Security Program is to ensure official information of the Department of the Navy relating to national security is protected to the extent and for a period of time as may be necessary. The *Department of the Navy Information and Personnel Security Program Regulation* establishes the basis for the identification of information to be protected; prescribes a progressive system for classification, downgrading, and declassification; prescribes safeguarding policies and procedures to be followed; and sets up a monitoring system to ensure the effectiveness of the program.

The Security Program basically deals with the safeguarding of information that cannot be known or made available to foreign governments or foreign nationals because of the threat that such information might be used to the detriment of the United States. The security of the United States in general, and of naval operations in particular, depends in part upon the success attained in the safeguarding of classified information.

Information may be compromised through careless talk, through actual subversion by enemy agents, by careless handling of classified material, and in various other ways.

Definitions

To clearly understand certain terms used in connection with security, a list of terms and definitions is presented in the following paragraphs.

ACCESS —The ability and opportunity to obtain knowledge or possession of classified information. An individual does not have access to classified information merely by being in a place where such information is kept, provided the security measures that are in effect prevent this individual from gaining knowledge or possession of such classified information.

CLASSIFICATION —The determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

CLASSIFIED INFORMATION —Official information that has been determined to require, in the interest of national security, protection against unauthorized disclosure.

CLASSIFIED MATERIAL —Any matter, document, product, or substance on or in which classified information is recorded or embodied.

CLEARANCE —An administrative determination by competent authority that an individual is eligible for access to classified information of a specific classification category.

COMPROMISE —The known or suspected exposure of classified information or material to an unauthorized person.

CUSTODIAN —An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding and accounting for classified information.

DOCUMENT —Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing cards and tapes; maps; charts; paintings; drawings; engravings; sketches; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.

DOWNGRADE —To determine that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree.

HANDLING —Preparation, processing, transmission, and custody of classified information.

MARKING —The physical act of indicating on classified material the assigned classification, changes in classification, downgrading and/or declassification instructions, and any limitations on use of the material.

NEED TO KNOW —The need for access to or possession of classified information to carry out official military or other governmental duties. Responsibility for determining whether a person's duties require that the person possess or have access to classified information and whether the person is authorized to receive it rests upon the possessor of the classified information and not upon the prospective recipient.

OFFICIAL INFORMATION —Information that is owned by, produced for or by, or is subject to the control of, the United States Government.

SECURITY —A protected condition of classified information that prevents unauthorized persons from

sobtaining information of direct or indirect military value. This condition results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

SECURITY VIOLATION —Any failure to comply with regulations relative to the security of classified material that does not result in compromise or subjection to compromise.

Q8. What description best defines the term access?

CATEGORIES OF CLASSIFIED INFORMATION

Official information or material that requires protection in the interest of national security must be classified in one of three categories, Top Secret, Secret, or Confidential, depending upon the degree of its significance to national security. No other categories may be used to identify official information or material as requiring protection in the interest of national security.

Top Secret

Top Secret is the designation that is applied only to information or material of which the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

Secret

Secret is the designation that is applied only to information or material of which the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or

technological developments relating to national security.

Confidential

Confidential is the designation that is applied to information or material of which the unauthorized disclosure could reasonably be expected to cause identifiable damage to national security. Examples of identifiable damage include the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas; the disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; and the revelation of performance characteristics, test data, design, and production data on munitions of war.

For Official Use Only

For Official Use Only is **NOT** a category of classification but is assigned to certain official information not within the range of the rules for safeguarding information in the interest of national security, but may require protection according to law or in the public interest.

Restricted Data or Formerly Restricted Data

Restricted Data, like For Official Use Only, is **NOT** a category of classification but is assigned because it concerns data (information) covering the (1) design, manufacture, or use of atomic or nuclear weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but not to include data declassified or removed from the Restricted Data category under Section 142 of the Atomic Energy Act. Formerly Restricted Data is information removed from the Restricted Data category upon determination jointly by the Department of Energy and DOD that such information relates primarily to the military use of atomic weapons and that such information can be adequately safeguarded as classified defense information. Such information is, however, treated the same as Restricted Data for purposes of foreign dissemination.

Material bearing the Restricted Data or Formerly Restricted Data warning notices may not be issued outside authorized channels without the permission of the originator or higher DOD authority. (Refer to the *Department of the Navy Information and Personnel Security Program Regulation*, OPNAVINST 5510.1.)

The Department of Energy grants two types of personnel clearances, L and Q, for access to classified information that includes Restricted Data. These clearances are not required by Navy personnel, provided they have been cleared for access to classified information at least equal to the classification category of the Restricted Data involved.

For further information concerning clearances for and issuance of Restricted Data or Formerly Restricted Data, refer to OPNAV instruction 5510.1.

Q9. The Navy Information and Personnel Security Program consists of what three information categories?

HANDLING CLASSIFIED INFORMATION

Each individual in the naval establishment must take every precaution to prevent deliberate or casual access to classified information by unauthorized persons. Some of the precautions to be taken are listed in the following paragraphs:

- When classified documents are removed from stowage for working purposes, they must be kept facedown or covered when not in use.

- Visitors not authorized access to particular classified information within a working space will be received or interviewed in specially arranged reception rooms or areas.

- Classified information will not be discussed over the telephone. Telephone scrambling devices do not assure security.

- Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, work sheets, and all similar items containing classified information will be either destroyed by the person responsible for their production immediately after the material has served its purpose or given the same classification and safeguarded in the same manner as the classified information produced from the material.

- Classified material, upon receipt, must be opened by the addressee or by persons specifically authorized by the addressee to open material of the classification involved.

If, for any reason, an office is vacated during working hours, the classified material therein will be stowed in the prescribed manner as if it were after working hours.

TRANSMISSION OF CLASSIFIED INFORMATION

By executive order, Secret and Confidential material may be transmitted outside CONUS by USPS registered mail through Army, Navy, or Air Force postal facilities, provided that the material does not at any time pass out of U.S. Government control and does not pass through a foreign postal system. Secret and Confidential material may be transmitted between the United States and/or Canadian Government installations in the United States, Canada, and Alaska, by United States and Canadian registered mail with a return receipt. Only closed pouches or jackets of registered U.S. mail may be transported between U.S. activities and overseas military post offices (MPOs). (See fig. 2-5.)

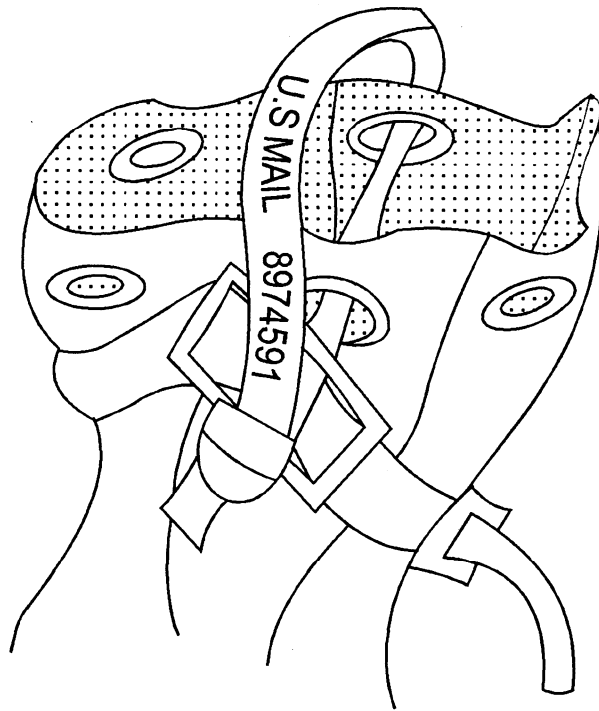
Closed pouches or jackets of registered U.S. mail, bearing an APO, FPO, or a CONUS address, maybe transported between U.S. activities by Canadian military or Canadian civil postal facilities without the individual requests for return receipt as required in the case of registered mail containing classified material addressed to Canadian geographic (international) addresses.

All classified material that is mailed at U.S. MPOs outside CONUS must be registered. All classified material that is mailed at post offices in CONUS addressed to an APO or FPO address will also be registered, since originators cannot know in the case of mobile units whether or not retransmission outside CONUS maybe required.

Q10. You are mailing a document marked Confidential from the Commander Naval Base, Norfolk, VA, to a ship with an FPO, AP address. What special category of mail should you use for this purpose?

Preparation of Packages for Transmission

Except for transmission locally within a ship or office, classified matter being mailed must be enclosed in opaque double-sealed containers or envelopes to minimize the possibility of compromise. Commands provide for the stocking of several sizes of cardboard containers, corrugated paper, and kraft tape laminated with asphalt and containing rayon fibers (snake tape), or nylon sensitive tape. COs will require the inspection of bulky packages to decide whether the material is



OMMPC008

Figure 2-5.—Example of a Registered Pouch or Jacket using a USPS registered tin band seal.

suitable for mailing or whether it should be sent by other approved means.

Destruction of Classified Material

Classified material is destroyed by burning or by pulping, provided destruction is complete and reconstruction is impossible. Equipment that bears a security classification is destroyed by smashing beyond recognition. Equipment may also be jettisoned in water of sufficient depth to prevent recovery.

Destruction bills of particular activities include lists that show the locations of classified material, personnel responsible for its destruction, and the recommended place and method of destruction. Classified material is destroyed during emergencies when there is danger that it may be compromised. Communication material receives first priority. Of all communication materials, cryptographic material is destroyed first. Generally, the order of destruction

follows the classification —the highest classified material is destroyed first.

Q11. When sent through the US. mail, Confidential material must be enclosed in an envelope or a container that is double-sealed to prevent what type of problem?

Q12. In addition to burning, what other methods may be used to destroy classified material?

SUMMARY

We discussed the physical security provided to all mail and the Information and Personnel Security Program as it applies to classified material sent in the mail. We also discussed the requirements for maintaining the security of mail and equipment, random inspections, probable cause searches, and what to do if a suspected letter or parcel bomb is found. Finally, we discussed the proper destruction of classified material.

ANSWERS TO EMBEDDED QUESTIONS

CHAPTER 2

- A1. MPS and USPS.*
- A2. U.S.flag certified cargo air carriers.*
- A3. PS Form 3977 and SF 700.*
- A4. At least annually.*
- A5. Letter and parcel.*
- A6. DOD Postal Manual.*
- A7. CNO.*
- A8. The opportunity and ability to obtain knowledge of classified information.*
- A9. Top Secret, Secret, and Confidential.*
- A10. Registered mail.*
- A11. Compromise.*
- A12. Pulping, smashing, and jettisoning.*